KPMG
cutting through complexity

HOW VALUABLE ARE POWER & UTILITIES BUSINESSES TO CYBER CRIMINALS?

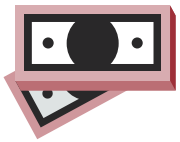
Cyber-crime is always high on the boardroom agenda for financial institutions and internet businesses globally, but surely power & utility executives can rest easy? After all, you can't steal electricity or water using a laptop. Think again.

According to news outlets, the Syrian Electronic Army (SEA) launched a successful cyber attack on the main infrastructure system of Haifa, one of the most important ports in Israel, disrupting the operation of the servers in charge of urban management systems and public utilities in the city.

TECHNOLOGY IS ONE OF THE MAIN INNOVATION AND GROWTH CATALYSTS IN POWER & UTILITIES. CYBER ATTACKS ON THE SECTOR'S SCADA SYSTEMS CAN IMPACT REVENUE, SAFETY AND HAVE MUCH WIDER REPERCUSSIONS

ACCORDING TO THE UK GOVERNMENT CYBER GOVERNANCE HEALTH CHECK, 2 OUT OF 3 CHAIRS OF THE FTSE350 EXPECT CYBER RISKS TO INCREASE, WITH AT LEAST 1 OUT OF 3 STATING THEY ARE "ANXIOUS" ABOUT THE THREAT

IN THE UK ALONE, CYBER ATTACKS COST SOME 27 BILLION POUNDS A YEAR, ACCORDING TO THE UK CABINET OFFICE



In a world where electricity and the security of supply is key to national infrastructure and critical for businesses to remain competitive in a global market, the power & utility industry and other operators of critical energy infrastructure, could find themselves vulnerable to having their cyber-security compromised. A really sophisticated cyber attack could cause a blackout bigger than ever seen in the UK which would be detrimental not only to the industry but to the national economy. The threat of state-sponsored cyber-warfare is not inconceivable either, particularly for an industry providing critical national infrastructure.

There are already examples of cyber-espionage to control energy and natural resources and given that these have been seen to be successful, many analysts see the use of cyber-espionage spreading. The 2012 attack on the world's largest exporter of crude, Saudi Aramco in which over 30,000 computers were compromised or affected, highlighted the potential impact a virus could have had on global hydrocarbon markets. The attack on Aramco points to an escalation in cyber-attacks, with the adversaries constantly upping their game in a cyber arms race.

Whilst there is no miraculous solution for keeping critical power & utility assets secure against today's evolving cyber threats, boards need to be on the front foot and devise holistic and robust strategies to be in the strongest position for dealing with the developing cyber landscape, focussing on creating better agility and providing the capabilities needed to counter threats as they evolve.

CYBER ATTACKS ARE EXPECTED TO SPUR SIGNIFICANT INVESTMENT IN CYBER-SECURITY BY 2018

The reality is that many businesses have a long way to go in catching up with cyber criminals.

Many businesses are taking this issue seriously and making significant investments strategically and financially, trying to stay ahead of the criminals.KPMG has helped firms transform their information risk and IT security functions to deal with the new world.

Our team includes engineers and IT security professionals who understand SCADA systems and work together with our clients to tackle this matter successfully.

To find out more about protecting your business from cyber criminals, visit www.kpmg.com/uk/cyber

CHARLES HOSNER

Partner
T: +44 (0) 20 7694 5801
E: charles.hosner@kpmg.co.uk